REMARKS

The Office Action dated May 4, 2005, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1 and 9-12 are amended to more particularly point out and distinctly claim the subject matter of the invention. No new matter is added. Thus, claims 1-14 are presently pending in the application and are respectfully submitted for consideration.

Applicant wishes to acknowledge with appreciation the courtesy extended to applicant's representative during the interview on July 29, 2005. As discussed below and indicated by the Examiner during the interview, the claims distinguish over the cited references.

Claims 1-6 and 9-11 were rejected under 35 U.S.C. §102(b) as allegedly anticipated by U.S. Patent No. 5,623,600 (Ji et al.). The Office Action took the position that Ji taught all the elements of claims 1-6 and 9-11. Applicant respectfully submits that Ji fails to disclose or suggest all the features of any of the presently pending claims.

Claim 1, upon which claims 2-6 are dependent, recites a method of scanning electronic files for computer viruses. The method includes identifying at a first node of a computer network, electronic files which are required to be scanned for computer viruses. The method also includes initiating a dialogue between the first node and a second node of the network. A second node includes a virus scanning application, during which dialogue the second node identifies to the first node one or more portions of the

electronic file required by the virus scanning application. The method also includes transferring the identified portions from the first node to the second node over the network. The method also includes, at the second node, scanning the transferred portions for computer viruses. The method also includes, if the second node determines that the electronic file includes a computer virus and determines that the electronic file is able to be disinfected, informing the first node by the second node of the determinations.

Claim 9 recites an anti-virus scanning system for use in scanning electronic files in a computer network. The system includes a first computer having processing means arranged to identify electronic files which should be scanned for computer viruses. The system also includes a second computer having processing means arranged to perform a virus scanning operation. The first computer further includes communication means for initiating a dialogue between the first computer and the second computer, during which the second computer identifies to the first computer those portions of the electronic files required by the first computer for performing the virus scanning operation, and for transferring those portions to the second computer. The second computer further includes determination means for scanning the transferred portions for computer viruses, and, when the second computer determines that the electronic files include a computer virus and determines that the electronic files are able to be disinfected, informing the first computer of the determinations.

Claim 10 recites a computer memory encoded with executable instructions representing a computer program for causing a first computer connected to a computer

network to identify an electronic file which is required to be scanned for computer viruses. The computer memory encoded with the executable instructions also causes a first computer connected to the computer network to initiate a dialogue between the first computer and a second computer also connected to the computer network. The computer memory encoded with the executable instructions also causes the first computer connected to the computer network to receive from the second computer an identification of portions of the electronic file which are required for virus scanning of the electronic file at the second computer. The computer memory encoded with the executable instructions also causes the first computer connected to the computer network to transfer the identified portions from the first computer to the second computer. The computer memory encoded with the executable instructions also causes the first computer connected to the computer network to scan the transferred portions for computer viruses at the second computer. The computer memory encoded with the executable instructions also causes the first computer connected to the computer network, if the second computer determines that the electronic file includes a computer virus and determines that the electronic file is able to be disinfected, to inform the first computer by the second computer of the determinations

Claim 11 recites a computer memory encoded with executable instructions representing a computer program for causing a first computer connected to a computer network to receive a dialogue initiation request from a second computer also connected to the computer network concerning an electronic file identified by the second computer as

requiring a virus scan. The computer memory encoded with the executable instructions also causes the first computer connected to the computer network to identify to the second computer those portions of the electronic file which are required by the first mentioned computer for performing a virus scanning operation at the first computer. The computer memory encoded with the executable instructions also causes the first computer connected to the computer network to receive the identified portions of the electronic file from the second computer. The computer memory encoded with the executable instructions also causes the first computer connected to the computer network to inform the second computer of an outcome if the first computer determines that the electronic file includes a computer virus and determines that the electronic file is able to be disinfected.

As discussed in the specification, examples of the present invention enable the identification by the second node to the first node of those portions of a file which are required by the second node to effectively scan the file for viruses. Thus, the scanning related intelligence located at the first node may rarely need updating. Further, examples of the present invention enable the use of electronic files that are required to be scanned for viruses to be identified at the first node, either client or agent. The second, or server, node identifies to the first node portions of the electronic file that are required to be sent to the second node. Thus, only the identified portions are sent. Traffic in the network and between the nodes may be reduced because the entire file does not have to be transferred. Applicant respectfully submits that Ji fails to disclose or suggest the

elements of any of the presently pending claims. Therefore, Ji fails to provide the critical and unobvious advantages discussed above.

Ji relates to a virus detection and removal apparatus for computer networks. Ji describes a memory 44 for a gateway node 33 having a File Transfer Protocol (FTP) proxy server 60, a Simple Mail Transfer Protocol (SMTP) proxy server 62, and an operating system 64 including a kernel 66. FTP proxy server 60 is a routine for controlling file transfers to and from gateway node 33 via communications unit 54, and thus controlling file transfers to and from a given network of which the gateway node is a part. SMTP proxy server 62 is a routine for controlling the transfer of messages to and from gateway node 33, and thus to and from the respective network associated with gateway node 33. Referring to Figure 6C of Ji, FTP proxy server 60, in step 646, determines whether a file to be transferred is of a type that can contain viruses. If the file to be transferred is a type that can contain viruses, step 650 of Ji temporarily stores the file at the gateway node. In step 652, the temporarily stored file is analyzed to determine if it contains viruses. If a virus is detected, Ji describes retrieving a configuration file to determine the handling of the temporary file. FTP proxy server 60 then determines if it is to ignore the existence of a virus and continue the file transfer or erase the stored file.

Applicant submits that Ji fails to disclose or suggest all the features of any of the presently pending claims. For example, Ji fails to disclose or suggest, if the second node determines that the electronic file includes a computer virus and determines that the electronic file is able to be disinfected, informing the first node by the second node of the

determinations. As discussed above, the FTP proxy server of Ji only determines if it is to ignore the virus or erase the file. Ji fails to inform another node or server that the file includes a computer virus and that the file is able to be disinfected. Applicant submits that Ji fails to determine whether the file can be disinfected, but only describes transferring or erasing the file if it has a virus.

In contrast, claim 1 recites "if the second node determines that the electronic file includes a computer virus and determines that the electronic file is able to be disinfected, informing the first node by the second node of the determinations." Claim 9 recites "the second computer further comprising determination means for scanning the transferred portions for computer viruses, and, when the second computer determines that the electronic files include a computer virus and determines that the electronic files are able to be disinfected, informing the first computer of the determinations." Claim 10 recites to, "if the second computer determines that the electronic file includes a computer virus and determines that the electronic file is able to be disinfected, inform the first computer by the second computer of the determinations." Claim 11 recites to "inform the second computer of an outcome if the first computer determines that the electronic file includes a computer virus and determines that the electronic file is able to be disinfected." Applicant maintains that Ji, for the reasons given above, fails to disclose or suggest at least these features of the presently pending claims.

With regard to the dependent claims, applicant asserts that they are distinguishable from Ji for the reasons give above and also because the dependent claims recite additional

patentable subject matter. Further, in the interview with the Examiner on July 29, 2005, it was indicated that the claims distinguish over Ji for the reasons given above. Thus, applicant respectfully requests that the anticipation rejection be withdrawn.

Claim 7 was rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Ji in view of U.S. Patent No. 5,832,208 (Chen et al.). The Office Action took the position that Ji taught all the features of claim 7 except transferring from the second node to the first node data portions to be written into the file to disinfect the file. The Office Action then alleged that Chen provided the features missing from Ji. Applicant respectfully submits that Ji and Chen, either alone or in combination, fail to disclose or suggest all the features of any of the presently pending claims.

Claim 7 depends from claim 1. Claim 1 is summarized above. Applicant submits that claim 7 includes the features of claim 1, as well as other features.

Ji is discussed above. Chen relates to an anti-virus agent for use with databases and mail servers. Chen describes a software agent for detecting and removing computer viruses located in attachments to email messages. A client-server computer network includes a server computer and a plurality of client computers. A message system, located at the server computer, controls the distribution of email messages. An anti-virus module, located at the server computer, scans files for viruses. The agent is located at the server computer and provides an interface between the anti-virus module and the message system. Email messages that are sent internally within the network can be scanned.

Applicant submits that Ji and Chen fail to disclose or suggest all the features of claim 7. As discussed above, Ji fails to disclose or suggest, if the second node determines that the electronic file includes a computer virus and determines that the electronic file is able to be disinfected, informing the first node by the second node of the determinations. Applicant asserts that Chen, either alone or in combination with Ji, fails to disclose or suggest the features missing from Ji. Chen describes an anti-virus module that scans files attached to emails for viruses. Chen fails to inform any of the computers in its network that the attached files are able to be disinfected. Thus, Chen fails to disclose or suggest the features missing from Ji. Applicant maintains that Ji and Chen, either alone or in combination, fail to disclose or suggest all the features of claim 7. Further, during the interview of July 29, 2005, it was indicated that claim 7 distinguishes over Ji and Chen for the reasons given above. Therefore, applicant respectfully requests that the obviousness rejection be withdrawn.

Claims 8 and 12-14 were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Ji in view of U.S. Patent No. 6,067,410 (Nachenberg). The Office Action took the position that Ji taught all the features of claims 8 and 12-14 except sending instructions from the second node to the first node to inform the first node how to disinfect the file. The Office Action alleged that Nachenberg provided the features missing from Ji. Applicant respectfully submits that Ji and Nachenberg, either alone or in combination, fail to disclose or suggest all the features of any of the presently pending claims.

Claim 8 depends from claim 1. Claim 1 is summarized above. Applicant submits that claim 8 includes the features of claim 1, as well as other features.

Claim 12, upon which claims 13 and 14 are dependent, recites a method of disinfecting an electronic file stored at a first node of a computer network, after the file has been identified as containing a virus by a virus scanning engine located at a second network node. The first node and the second node initiate a dialogue. The method includes informing the first node by the second node that a virus has been identified and is able to be disinfected. The method also includes sending from the second node to the first node, data portions to be written into the infected file or instructions for disinfecting the file. The method also includes receiving the data portions or instructions at the first node and routing the data portions into the infected file or carrying out the instructions.

Ji is discussed above. Nachenberg relates to an emulation repair system. Nachenberg describes restoring virus-infected computer files to their uninfected states without risk of infecting the rest of the computer system by providing a virtual machine for emulating the virus-infected computer file, a foundation module including generic machine language repair routines and a virus specific overlay module. The emulation repair system receives the identity of the infected computer file and the infecting virus from a virus scanning module and uses the received information to access a virus definition that includes decryption information on the identified virus. The infected computer file is emulated in the virtual machine until it is determined from comparison with the decryption information that the virus is fully decrypted.

Applicant submits that Ji and Nachenberg, either alone or in combination, fail to disclose or suggest all the features of any of the pending claims. For example, Ji and Nachenberg fail to disclose or suggest informing the first node by the second node that a virus has been identified and is able to be disinfected. As discussed above, Ji fails to disclose or suggest these features of the claims. Applicant submits that Nachenberg, either alone or in combination with Ji, fails to disclose or suggest the features missing from Ji. Nachenberg describes providing a virtual machine for emulating the virus infected file. The emulation repair system of Nachenberg receives the identity of the infected computer file and the infecting virus and uses this information to access a virus definition. Nachenberg, however, fails to disclose or suggest informing a first node by a second node if the second node determines that the electronic file includes a computer virus and determines that the electronic file is able to be disinfected.

In contrast, claim 8 depends from claim 1, which recites "if the second node determines that the electronic file includes a computer virus and determines that the electronic file is able to be disinfected, informing the first node by the second node of the determinations." Claim 12 recites "informing the first node by the second node that a virus has been identified and is able to be disinfected." Applicant maintains, for the reasons given above, that Ji and Nachenberg fail to disclose or suggest at least these features of the pending claims.

With regard to the dependent claims, applicant asserts that they are distinguishable from Ji and Nachenberg for the reason given above, and because the dependent claims

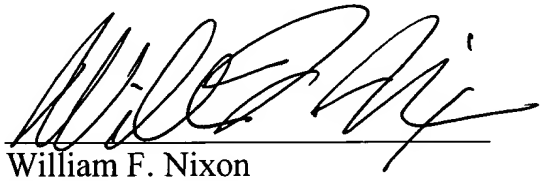
recite additional patentable subject matter. Further, in the interview of July 29, 2005, it was indicated that the claims are distinguishable over Ji and Nachenberg. Therefore, applicant respectfully requests that the obviousness rejection be withdrawn.

It is further submitted that each of claims 1-14 recites subject matter that is neither disclosed nor suggested by Ji, Chen and Nachenberg, either alone or in combination. It is therefore respectfully requested that all of claims 1-14 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



William F. Nixon
Registration No. 44,262

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

WFN:cct